Social media OSINT

STAGE :- 1

Definition :-

“Social Media Reconnaissance, often used in Open-Source Intelligence (OSINT), involves gathering publicly available information from social media platforms. Here's a breakdown of the listed activities”

1. Profiling Individuals or Organizations

Purpose:- To understand an entity's online presence, behavior, and influence.

Techniques:-

1. Review public profiles for biographical data (location, occupation, interests).
2. Analyze post frequency, tone, and content type.
3. Identify recurring themes or causes the individual/organization supports.
4. Use tools like Maltego or Sherlock to consolidate profiles across platforms.

2. Tracking Social Activity and Interactions

Purpose: Monitor engagement and interactions to gauge influence and network reach.

Techniques:

1. Track likes, shares, and comments to determine engagement levels.
2. Monitor hashtags, mentions, and trending topics related to the entity.
3. Use tools like Hootsuite or Mentionlytics for comprehensive monitoring.

3. Identifying Connections, Groups, and Networks

Purpose: Map relationships to uncover networks or potential affiliations.

Techniques:

1. Analyze friend lists, followers, and mutual connections.
2. Look for participation in public groups, forums, or events.
3. Use network analysis tools (e.g., Gephi or NodeXL) to visualize connections.

4. **Extracting Metadata from Shared Posts and Images**

Purpose: Gather hidden data (e.g., timestamps, geolocation) to derive additional insights.

Techniques:

1. Extract EXIF data from images for location and device information (using tools like ExifTool).
2. Analyze timestamps and frequency of posts to identify patterns.
3. Use online tools or scripts to scrape metadata were allowed by the platform's terms of service

Stage :- 2

TYPE OF OSINT

1. Passive OSINT
2. Active OSINT

Passive OSINT

Definition

"Involves collecting information without interacting directly with the target, minimizing detection risk."

Techniques & Tools

1. Public Profile Analysis

Platforms: Twitter, LinkedIn, Instagram, Facebook.

Tools:-

1. Sherlock: Searches for usernames across platforms.
2. Social-Searcher: Searches public social media content by keyword.

3. Pipl: Finds profiles using names, emails, or usernames.

2. **Metadata Extraction**

Extract metadata from public posts or images.

Tools:

1. ExifTool: Extracts EXIF data from photos for geolocation and device details.
2. OSINT Combine Metadata Tools: Collects metadata from various sources.

3:- **Network Mapping**

Create a map of connections using publicly available information.

Tools:-

1. Maltego:- Builds relationships and networks from open data.
2. SpiderFoot:- Gathers data across multiple sources, including social media.

4**. Social Media Monitoring**

Monitor public discussions, hashtags, or posts.

Tools:

1. Hootsuite: Tracks mentions and keywords on platforms.
2. Mentionlytics: Monitors social mentions and sentiments.

Active Reconnaissance

Definition:-

Involves engaging directly with the target (e.g., sending connection requests, commenting). May increase detection risk.

Techniques & Tools

1. **Direct Engagement**

Interact with posts or send direct messages to gather more details.

Example: Engage in discussions on LinkedIn or join public Facebook groups.

2. Connection Requests

“Send connection requests on LinkedIn, Facebook, or Instagram to access restricted data.”

Tools:

Manual platform uses or browser automation (e.g., Selenium).

3. Advanced Search Queries

“Use search operators for deeper data retrieval.”

Tools:

1. Google Dorking: Combines advanced search operators for better results.
2. Recon-ng: Automates OSINT tasks, including social media searches.

4. Post Analysis

Engage with posts to solicit information or observe responses.

Example: Ask open-ended questions in a comment section.

Recommended Tools

General OSINT Tools for both purpose

1. Maltego: Network and relationship mapping.
2. SpiderFoot: Comprehensive OSINT automation.
3. Recon-ng: Social media and other OSINT modules.
4. Social Media-Specific Tools
5. SocioSpyder: Social media scraping and monitoring.
6. Twint: Twitter scraping tool for public data.
7. IntelTechniques Tools: Social media search and analysis.
8. Metadata and Image Analysis
9. ExifTool: Extract metadata from media files.
10. PhotoDNA: Identifies image origins and potential tampering.

Practical approach for social media osint

1. **Definition:-**

Goal: Understand the purpose of the investigation.

1. Identify targets (individuals, organizations, or groups).
2. Specify the type of data you're looking for (e.g., connections, activities, metadata).

2. **Data Collection**

A**. Identify Target Accounts**

Tool:-

1. Sherlock: Finds usernames across multiple platforms.
2. Namechk: Checks username availability.

B. Public Profile Analysis

Platforms:-

a) Facebook: Groups, likes, photos, comments.
b) Twitter: Tweets, followers, hashtags, mentions.
c) LinkedIn: Professional details, endorsements, connections.
d) Instagram: Posts, stories, followers, geotags.

Tools:

1. Twint: Scrapes Twitter data without API limits.
2. SocioSpyder: Scrapes data from multiple platforms.

C. Network Mapping

Create a map of relationships and connections.

Tools:

1. Maltego: Graphical network analysis.
2. SpiderFoot: Automates discovery of links and relationships.

D. Metadata Extraction

Extract metadata from images, posts, and videos.

Tools:

1. ExifTool: Extracts geolocation, timestamps, and device info.
2. Hunchly: Captures and organizes online investigations.

3. Analyze Social Media Behavior

Content Analysis:

Identify frequent topics or hashtags.

Tools: NodeXL (analyzes social media networks and content).

4.Sentiment Analysis:

Determine the tone and emotion of posts.

Tools: MonkeyLearn, Lexalytics.

5.Engagement Analysis:

Track likes, shares, and comments to gauge influence.

Tools: Hootsuite, Mentionlytics.

6. Investigate Connections and Networks

Follower/Following Analysis:

Identify key followers or mutual connections.

Tools: Followerwonk (Twitter analysis).

7.Group Participation:

Look for group memberships on Facebook, LinkedIn, etc.

Tools: IntelTechniques Facebook Tools.

8. Report Preparation

Summarize findings in a structured report:

Key observations.

Evidence (screenshots, metadata, network graphs).

Conclusions and actionable insights.

Ethical and Legal Considerations

Respect privacy laws and platform terms of service.

Avoid accessing unauthorized or private information. 1. Define Objectives

Goal: Understand the purpose of the investigation.

Identify targets (individuals, organizations, or groups).

Specify the type of data you're looking for (e.g., connections, activities, metadata).

2. Data Collection

A. Identify Target Accounts

Use tools like:

Sherlock: Finds usernames across multiple platforms.

Namechk: Checks username availability.

B. Public Profile Analysis

Platforms:

- Facebook: Groups, likes, photos, comments.
- Twitter: Tweets, followers, hashtags, mentions.
- LinkedIn: Professional details, endorsements, connections.
- Instagram: Posts, stories, followers, geotags.

Tools:

Twint: Scrapes Twitter data without API limits.

SocioSpyder: Scrapes data from multiple platforms.

C. Network Mapping

Create a map of relationships and connections.

Tools:

Maltego: Graphical network analysis.

SpiderFoot: Automates discovery of links and relationships.

D. Metadata Extraction

Extract metadata from images, posts, and videos.

Tools:

ExifTool: Extracts geolocation, timestamps, and device info.

Hunchly: Captures and organizes online investigations.

3. Analyze Social Media Behavior

A. **Content Analysis:**

Identify frequent topics or hashtags.

Tools: NodeXL (analyzes social media networks and content).

B. **Sentiment Analysis:**

Determine the tone and emotion of posts.

Tools: MonkeyLearn, Lexalytics.

C. **Engagement Analysis:**

Track likes, shares, and comments to gauge influence.

Tools: Hootsuite, Mentionlytics.

4. Investigate Connections and Networks

1) Follower/Following Analysis:
2) Identify key followers or mutual connections.
3) Tools: Followerwonk (Twitter analysis).
4) Group Participation:
5) Look for group memberships on Facebook, LinkedIn, etc.
6) Tools: IntelTechniques Facebook Tools.

5. Use Advanced Techniques

A. Google Dorking

Use advanced search operators to find public social media data.

Example: site:facebook.com "John Doe" "New York"

B. Image and Video Analysis

Perform reverse image searches and verify image authenticity.

Tools:

1. Google Reverse Image Search.
2. InVID: Video verification tool.
3. PhotoDNA: Image analysis.

C. Geolocation

Identify locations from photos or posts.

Tools:

1. GeoSocial Footprint: Analyzes location-based social media activity.

2. Mapillary: Crowd-sourced street-level imagery.

6. Document Findings

Use tools to organize and visualize collected data:

CaseFile: Simple relationship mapping.

Hunchly: Organizes and saves online investigations.

7. Evaluate and Corroborate

1. Cross-check information across multiple sources for accuracy.
2. Verify the authenticity of profiles and posts.

8. Report Preparation

Summarize findings in a structured report:

Key observations :-

1. Evidence (screenshots, metadata, network graphs).
2. Conclusions and actionable insights.

Dorks for social media osint and investigation

1. General Social Media Dorks

A. **Search for Profiles**

Find profiles by name:

1. site:facebook.com "John Doe"
2. site:twitter.com "John Doe"
3. site:instagram.com "John Doe"
4. site:linkedin.com "John Doe"

B. **Search for usernames:**

1. site:twitter.com inurl:username
2. site:instagram.com inurl:username

C. **Search for Emails**

Find profiles with email IDs

1. site:facebook.com "@gmail.com"
2. site:twitter.com "@yahoo.com"

D. Search for Keywords in Posts

Find posts with specific terms:

1. site:twitter.com "hacking"
2. site:facebook.com "cybersecurity"

2. Facebook Dorks

1) **Public Posts**

Posts with specific keywords:

1. site:facebook.com inurl:posts "vacation in Paris"
2. site:facebook.com inurl:posts "cybersecurity tips"

Groups

Find Facebook groups by topic:

site:facebook.com inurl:groups "travel"

Photos

1. Search for public photos:
2. site:facebook.com inurl:photos "John Doe"

3. Twitter Dorks

A) Tweets

Find tweets with specific phrases:

site:twitter.com intext:"OSINT techniques"

B) Hashtags

Search for specific hashtags:

site:twitter.com "#opsec"

C) **Mentions**

Find mentions of a username or keyword:

site:twitter.com "@username"

4. Instagram Dorks

A) Photos

Search for Instagram profiles or photos:

site:instagram.com "John Doe"

site:instagram.com inurl:photos

B) Hashtags

Find Instagram posts with specific hashtags:

site:instagram.com "#foodie"

5. LinkedIn Dorks

A) Profiles

Search for professionals by name:

site:linkedin.com "Jane Smith"

B) Job Titles

Find people with specific job titles:

site:linkedin.com "Cybersecurity Analyst"

C) Companies

Search employees of a company:

site:linkedin.com "employees at Google"

6. Other Useful Dorks

Search by Location

Find profiles by city:

site:facebook.com "John Doe" "New York"

Find Leaked Credentials

A) Search for leaks involving emails or passwords:

1. intext:"@gmail.com" filetype:txt
2. intext:"password" filetype:xls

Usage Tips

Combine multiple operators for precise results. Example:

1) site:twitter.com "Jane Doe" "#cybersecurity" -filter:retweets

Use time-based filters to narrow down results. Example:

2) site:facebook.com "John Doe" after:2023